AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of the Claims:

1.   (Currently Amended) A method of indicating signature status and trust status of a secure message on a messaging client, the method comprising the steps of:

selecting for processing a secure message stored on the messaging client, the secure message including a digital signature generated by a sender of the secure message;

checking the digital signature;

checking trust status of the sender;

displaying a first indicator of a result of the step of checking the digital signature; and

displaying a second indicator of a result of the step of checking trust status of the sender;

wherein:

the secure message includes a message body;

the method further comprises the step of processing the message body;

the step of checking the digital signature comprises determining whether the digital signature is valid or invalid;

the step of checking trust status comprises determining whether the sender is trusted or untrusted; and

the step of processing is performed only if the digital signature is valid and the sender is trusted.

2-4.   (Canceled)

5.   (Currently Amended) The method of claim 2̶1, wherein the step of processing the secure message comprises displaying the message body on a display screen on the messaging client.

6.   (Currently Amended) The method of claim 3̶1, wherein the first indicator includes a valid signature indication and an invalid signature indication.

7.   (Original)   The method of claim 6, wherein the second indicator includes a trusted indication and an untrusted indication.

8.   (Original)   The method of claim 7, wherein the first and second indicators comprise an icon.

9.   (Original)   The method of claim 7, wherein the first and second indicators comprise text.

10.   (Original)   The method of claim 8, wherein the first and second indicators further comprise text.

11.   (Original)   The method of claim 10, wherein the second indicator comprise a plurality of untrusted indications.

12. (Original) The method of claim 11, wherein the plurality of untrusted indications includes an invalid Certificate (Cert) indication, a revoked Cert indication, a missing Cert indication, and an expired Cert indication.

13. (Currently Amended) The method of claim ~~3~~1, wherein:

the digital signature includes a digest and a digest signature; and

the step of checking the digital signature comprises the steps of:

generating a digest of a message body of the secure message;

extracting a digest from the digital signature;

comparing the generated and extracted digests;

checking a digest signature in the digital signature to determine if the digest signature is valid or invalid; and

determining that the digital signature is valid when the generated and extracted digests match and the digest signature is valid.

14. (Currently Amended) The method of claim ~~3~~1, wherein:

the secure message also includes a Certificate (Cert) of the sender, the Cert including sender identity information and a public key bound to the sender identity information by a Cert signature generated by an issuer of the Cert; and

the step of checking trust status of the sender comprises the steps of:

checking the Cert signature to determine if the Cert signature is valid or invalid;

if the Cert signature is invalid, then determining that the sender is untrusted; and

if the Cert signature is valid, then

determining whether the issuer of the Cert is a trusted entity;

if the issuer is a trusted entity, then determining that the sender is trusted;

if the issuer is not a trusted entity, then

repeating the steps of checking the Cert signature and determining whether the issuer of the Cert is a trusted entity for each Cert in a Cert chain associated with the Cert of the sender to determine if a valid certification path to a valid root Cert from a trusted entity exists in the chain; and

if a valid certification path to a valid root Cert exists in the chain, then determining that the sender is trusted.

15.   (Original)   The method of claim 14, wherein:

the step of checking trust status of the sender further comprises the steps of:

determining if the Cert of the sender is missing from the secure message and if so, determining that the sender is untrusted;

determining if the Cert of the sender is expired and if so, determining that the sender is untrusted; and

checking a Certificate Revocation List (CRL) to determine if the Cert of

the sender has been revoked and if so, determining that the sender is untrusted;

and

the step of repeating the steps of checking and determining further comprises

repeating the steps of determining if a Cert is expired and checking a CRL.

16.   (Original)   The method of claim 1, wherein the messaging client is operating on a

wireless mobile communication device.

17.   (Original)   The method of claim 1, wherein the messaging client is operating on a

personal computer system.

18-22. (Canceled)

23.   (New) A method of indicating signature status and trust status of a secure message on a

messaging client, the method comprising the steps of:

selecting for processing a secure message stored on the messaging client, the

secure message including a digital signature generated by a sender of the secure message;

checking the digital signature;

checking trust status of the sender;

displaying a first indicator of a result of the step of checking the digital signature;

and

displaying a second indicator of a result of the step of checking trust status of the sender;

wherein:

the secure message includes a message body;

the method further comprises the step of processing the message body;

the step of checking the digital signature comprises determining whether the digital signature is valid or invalid;

the step of checking trust status comprises determining whether the sender is trusted or untrusted; and

the first indicator includes a valid signature indication and an invalid signature indication.

24. (New) The method of claim 23, wherein the step of processing the secure message comprises displaying the message body on a display screen on the messaging client.

25. (New) The method of claim 23, wherein the second indicator includes a trusted indication and an untrusted indication.

26. (New) The method of claim 25, wherein the second indicator comprises a plurality of untrusted indications.

27.   (New) The method of claim 26, wherein the plurality of untrusted indications includes an invalid Certificate (Cert) indication, a revoked Cert indication, a missing Cert indication, and an expired Cert indication.

28.   (New) The method of claim 23, wherein:

the digital signature includes a digest and a digest signature; and

the step of checking the digital signature comprises the steps of:

generating a digest of a message body of the secure message;

extracting a digest from the digital signature;

comparing the generated and extracted digests;

checking a digest signature in the digital signature to determine if the digest signature is valid or invalid; and

determining that the digital signature is valid when the generated and extracted digests match and the digest signature is valid.

29.   (New) The method of claim 23, wherein:

the secure message also includes a Certificate (Cert) of the sender, the Cert including sender identity information and a public key bound to the sender identity information by a Cert signature generated by an issuer of the Cert; and

the step of checking trust status of the sender comprises the steps of:

checking the Cert signature to determine if the Cert signature is valid or invalid;

if the Cert signature is invalid, then determining that the sender is untrusted; and

if the Cert signature is valid, then

determining whether the issuer of the Cert is a trusted entity;

if the issuer is a trusted entity, then determining that the sender is trusted;

if the issuer is not a trusted entity, then

repeating the steps of checking the Cert signature and

determining whether the issuer of the Cert is a trusted entity for

each Cert in a Cert chain associated with the Cert of the sender to

determine if a valid certification path to a valid root Cert from a

trusted entity exists in the chain; and

if a valid certification path to a valid root Cert exists in the

chain, then determining that the sender is trusted.

30. (New) The method of claim 29, wherein:

the step of checking trust status of the sender further comprises the steps of:

determining if the Cert of the sender is missing from the secure message

and if so, determining that the sender is untrusted;

determining if the Cert of the sender is expired and if so, determining that

the sender is untrusted; and

checking a Certificate Revocation List (CRL) to determine if the Cert of

the sender has been revoked and if so, determining that the sender is untrusted;

and

the step of repeating the steps of checking and determining further comprises

repeating the steps of determining if a Cert is expired and checking a CRL.

31.   (New) A method of indicating signature status and trust status of a secure message on a

messaging client, the method comprising the steps of:

selecting for processing a secure message stored on the messaging client, the

secure message including a digital signature generated by a sender of the secure message;

checking the digital signature;

checking trust status of the sender;

displaying a first indicator of a result of the step of checking the digital signature;

and

displaying a second indicator of a result of the step of checking trust status of the

sender;

wherein:

the secure message includes a message body;

the method further comprises the step of processing the message body

the step of checking the digital signature comprises determining whether the

digital signature is valid or invalid;

the step of checking trust status comprises determining whether the sender is

trusted or untrusted;

the digital signature includes a digest and a digest signature; and

the step of checking the digital signature comprises the steps of:

generating a digest of a message body of the secure message;

extracting a digest from the digital signature;

comparing the generated and extracted digests;

checking a digest signature in the digital signature to determine if the

digest signature is valid or invalid; and

determining that the digital signature is valid when the generated and

extracted digests match and the digest signature is valid.

32.   (New) A method of indicating signature status and trust status of a secure message on a

messaging client, the method comprising the steps of:

selecting for processing a secure message stored on the messaging client, the

secure message including a digital signature generated by a sender of the secure message;

checking the digital signature;

checking trust status of the sender;

displaying a first indicator of a result of the step of checking the digital signature;

and

displaying a second indicator of a result of the step of checking trust status of the

sender;

wherein:

the secure message includes a message body;

the method further comprises the step of processing the message body

the step of checking the digital signature comprises determining whether the digital signature is valid or invalid;

the step of checking trust status comprises determining whether the sender is trusted or untrusted;

the secure message also includes a Certificate (Cert) of the sender, the Cert including sender identity information and a public key bound to the sender identity information by a Cert signature generated by an issuer of the Cert; and

the step of checking trust status of the sender comprises the steps of:

checking the Cert signature to determine if the Cert signature is valid or invalid;

if the Cert signature is invalid, then determining that the sender is untrusted; and

if the Cert signature is valid, then

determining whether the issuer of the Cert is a trusted entity;

if the issuer is a trusted entity, then determining that the sender is trusted;

if the issuer is not a trusted entity, then

repeating the steps of checking the Cert signature and determining whether the issuer of the Cert is a trusted entity for each Cert in a Cert chain associated with the Cert of the sender to determine if a valid certification path to a valid root Cert from a trusted entity exists in the chain; and

if a valid certification path to a valid root Cert exists in the chain, then determining that the sender is trusted.

33.   (New) A system for indicating signature status and trust status of a secure message on a messaging client, the system comprising:

means for selecting for processing a secure message stored on the messaging client, the secure message including a digital signature generated by a sender of the secure message;

means for checking the digital signature;

means for checking trust status of the sender;

means for displaying a first indicator of a result of the step of checking the digital signature; and

means for displaying a second indicator of a result of the step of checking trust status of the sender;

wherein:

the secure message includes a message body;

the system further comprises means for processing the message body

the means for checking the digital signature comprises means for determining whether the digital signature is valid or invalid;

the means for checking trust status comprises means for determining whether the sender is trusted or untrusted; and

said processing of the message body is performed only if the digital signature is valid and the sender is trusted.